AO 106 (Rev. 06/09) Application for a Search Warrant

# UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **semaj220@icloud.com** THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC. | Case No. 4:21 MJ 307 DDN<br>*Signed and Submitted to the Court for filing by reliable electronic means*<br>**FILED UNDER SEAL** |

## APPLICATION FOR A SEARCH WARRANT

I, Jack Hamil , a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

INFORMATION ASSOCIATED WITH **semaj220@icloud.com** THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.

located in the Northern District of California, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

✓evidence of a crime;
contraband, fruits of crime, or other items illegally possessed;
property designed for use, intended for use, or used in committing a crime;
a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| Title 18, U.S.C., §§ 1343 | Wire Fraud |

The application is based on these facts:
SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

✓ Continued on the attached sheet.
❑ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under penalty of perjury that the forgoing is true and correct

Thomas Hamil, Special Agent
United State Secret Service

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 28th day of October.

Date: ~~September XX, 2021~~ **Oct. 28, 2021** **/s/ David D. Noce**
*Judge's signature*

City and State: St. Louis, MO Honorable David D. Noce, U.S. Magistrate Judge
*Printed name and title*

AUSA: Derek J. Wiseman

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

| | | |
|---|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **semaj220@icloud.com** THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC. | ) | Case No. 4:21 MJ 307 DDN<br>*Signed and Submitted to the Court for filing by reliable electronic means*<br><br>**FILED UNDER SEAL** |

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Thomas Jack Hamil, a Special Agent with the United States Secret Service, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Apple Inc. (hereafter "Apple"), an electronic communications service/remote computing service provider, to disclose to the United States records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the United States Secret Service, and have been since June 2020. I received thirteen weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia. During this time, I was instructed in constitutional law pertinent to federal criminal investigations, arrest procedures, basic computer forensics, combat techniques, raid tactics, and the identification of contraband. Upon graduation from the Federal Law Enforcement

Training Center, I attended the United States Secret Service's training academy, known as the James J. Rowley Training Center, located in Beltsville, Maryland. During the course of my training there, I was instructed further in constitutional law, as well as Secret Service specific investigative subjects, to include the identification of counterfeit currency and documents, common fraud tactics, advanced electronic crime investigations, and interview techniques. This training also specifically included the investigation of financial crimes, identity theft, and "BICEP", a course covering the investigation of computer crime and fraud, network structures, and computer systems. Prior to becoming a Special Agent, I served as a police officer with the Saint Louis Metropolitan Police Department in St. Louis, Missouri, from August 27, 2017, until June 22, 2020. During my time with the Saint Louis Metropolitan Police Department, I was trained to investigate a variety of criminal matters, including "street crimes" – such as burglary, drug dealing, and fraud. I conducted numerous interviews and arrest operations, and assisted detectives in their investigations, including investigations of homicides, organized drug dealing, rape, and identity theft. Further, I authored affidavits, executed search warrants for, and seized electronic devices with the assistance of the St. Louis Metropolitan Police Department's cybercrimes division. Over the course of my career with the Saint Louis Metropolitan Police Department, I was issued three commendations for exceptional service; one for assisting the Intelligence Division with identifying and compiling a dossier on an individual threatening a politician, one for assisting paramedics in handling a knife-wielding subject, and a medal and associated commendation for "Valor in Service" for my actions during widespread civil unrest on June 1, 2020.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 USC 1343 have been committed by Semaj Portis. There is also probable cause to search the location described in Attachment A for the information described in Attachment B for evidence of these crimes.

## JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## LOCATION TO BE SEARCHED

6. The location to be searched is: **semaj220@icloud.com** (hereinafter referred to as "**the account(s)**") located at a premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

## BACKGROUND INFORMATION RELATING TO APPLE ID AND iCLOUD[1]

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

7. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

8. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the

user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

9. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

10. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

11. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

12. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs"

for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

13. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

14. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS")

messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

15. In some cases, account users will communicate directly with a Apple about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Apple typically retains records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

## PROBABLE CAUSE

16. The ERAP (Emergency Rental Arrears Program) is a program administered by the State of Missouri offering housing assistance for landlords who have renters with past-due rent. Landlords are the only ones who can apply for ERAP. The money disbursed through ERAP is sent directly to the landlords.

17. The SAFHR (State Assistance for Housing Relief) program is also a program administered by the State of Missouri offering housing assistance for landlords who have renters with past-due rent. Both landlords and tenants can apply. The money is disbursed directly to landlords, much like the ERAP program.

18. Both of the above-referenced programs are offered by the Missouri Housing Development Commission (MHDC). Both programs utilize federal aid being sent to the MHDC,

which is subsequently disbursed to the recipients based on the successful completion of an application process.

19. Between January 1, 2021, and present, 39 fraudulent SAFHR and ERAP applications associated with Semaj Portis were electronically submitted to the MHDC. On 22 of those applications, under the "Landlord Information" sections of the applications, Semaj Porter is named as the landlord, utilizing either her own name or the business name of her non-profit, Forever Riding. Under the "Application Point of Contact" sections in those same applications, Portis is listed as the point of contact, with an email address of **semaj220@icloud.com** (**the account**) and the phone number of 314-337-3116. On the other 17 applications, Forever Riding is listed as the landlord. It should be noted that Forever Riding is a business listed by the Missouri Secretary of State's records as being incorporated on January 15, 2021, with the registered agent being Semaj Porter (Semaj Portis' maiden name).

20. During this investigation, investigators have conducted interviews with many of the purported tenants listed in the fraudulent applications submitted to the MHDC listing Portis as a landlord and listing **the account** as her contact information. In addition, investigators have also analyzed property records for the properties included in those fraudulent applications. Based on this investigation, investigators have discovered that Portis was not, in fact, the landlord for the properties listed in the fraudulent applications that were submitted to the MHDC (in which her contact information included **the account** as her email address).

21. According to a representative from the MHDC, the MHDC frequently sends messages to the email addresses listed in the SAFHR and ERAP rental assistance applications. These messages from the MHDC can include notification of additional documentation requirements, payment/disbursement of funds, or any issues with the applications. Therefore, there

is probable cause to believe that that MHDC sent messages regarding the fraudulent applications to **the account**.

22. From my training and experience, I know it is common for individuals to store common contacts in email accounts in the form of email addresses and phone numbers, along with calendar dates, and financial information.

23. During a proffer interview with Portis and her attorney, Portis denied filing any applications to the MHDC. According to Portis, someone else submitted the applications, which included her name and contact information (including **the account** as her email address), and she did not know the fraudulent nature of the applications.

24. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

25. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

26. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs,

documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

27. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

28. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

29. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

## INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

30. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the United States copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## CONCLUSION

31. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

33. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under penalty of perjury that the forgoing is true and correct

Respectfully submitted,

SA

Thomas Jack Hamil
Special Agent
United States Secret Service

Subscribed and sworn to before me by reliable electronic means on October 28th, 2021.

**/s/ David D. Noce**
DAVID D. NOCE
UNITED STATES MAGISTRATE JUDGE

# ATTACHMENT A

## Property to Be Searched

This warrant applies to information associated with **semaj220@icloud.com** (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

# ATTACHMENT B

**Particular Things to be Seized**

**I.** iMessages, emails, and contacts sent or received by Semaj Porter, under the account name semaj220@icloud.com, relating to the matter at hand, including communication between semaj220@icloud.com and the associated account owner and the Missouri Housing Development Commission or representatives thereof;

**II.** Email attachments related to the same;

**III.** Calendar data or iCloud Drive documents, photos, or videos related to the same;

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique

Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account **01/01/2021 to present**, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account **01/01/2021 to present**, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including

Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

**The Provider is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.**

## IV. Information to be seized by the United States

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 USC 1343 involving Semaj Portis from 01/01/2021 to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.